

Definitions Associated with Prevention Tasks June 2003

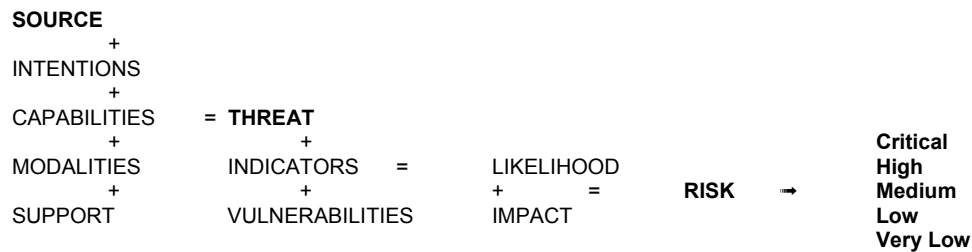
Analytical Models as examples for Assessing Risk/Vulnerability

(1) *Risk Management Model*, as described in David Schwendiman's, LECC Olympic Initiative Miscellaneous Paper No. 5 "Managing Intelligence In Multi-Jurisdiction Multi-Task Law Enforcement Environments: May 2002" pp.16-17:

- The components of a basic risk management analytical model Include:
 - (1) identifying the people and groups that are potential sources of criminal conduct or, in other words, security hazards;
 - (2) researching and understanding the historic intentions of any potential source;
 - (3) determining what the modalities and capabilities of the source are and determining whether he, she or they have access to materials, etc. to make either possible, (e.g. if the group or individual has demonstrated a preference for using pipe bombs in the past (modality) does he or she currently have access to the gunpowder, pipe, and expertise (capabilities) needed to carry out a pipe bombing or is he or she in a position to be able to acquire same?);
 - (4) evaluating the threat source's intentions in light of the person's or groups' modalities and capabilities to give a reasonable measure of the threat posed by the source, e.g., credible threat, not a credible threat;
 - (5) determining through all available collection sources and methods what the present indications are that the source is going to act according to his, her or the group's intentions, modalities and capabilities;
 - (6) if there are indicators, the questions become very specific: who precisely? where? what? when? how? What are the vulnerabilities, including an assessment of the state of readiness to deal with the source and its modalities and capabilities in the places, under the conditions, suggested by the indicators;
 - (7) the result is a measure of the likelihood that something will occur and may require a warning, that is, an alert, or an advisory;
 - (8) examining the impact of the expected action; and,
 - (9) calculating the resultant risk.

In this model, the "Risk is ranked according to a likelihood/impact index, i.e., the greater the risk on the matrix, the higher the risk is ranked. Taking each ranked risk, the decision maker either accepts the risk or engages in creating or deploying countermeasures designed to bring the result on the likelihood/impact matrix to an acceptable level by addressing those features in the analysis that can be controlled. Use of countermeasures is also informed by the potential consequences associated with employing them."

Without going into the details of the analytical model, it is diagramed in the referenced document as:



(2) *ODP Assessment Model* – This model uses a four step “vulnerability process” to assess risk. Step 1 is the Formation of the Planning Team, representing a broad array of organizations and disciplines. Step 2 requires that the Planning Team compile a list of the “most important” facilities, sites, systems, or special event activities that are present or take place within the jurisdiction. Step 3 involves individual vulnerability assessments of the individual targets, using seven Vulnerability Assessment Factors:

- Level of Visibility
- Criticality of Target Site
- Value of Target to Potential Threat Element (PTE)
- Potential Threat Element (PTE) Access to the Target
- Threat of Hazard
- Potential for Collateral Mass Casualty
- Site Population Capacity

The seven factors, their definitions, and associated rating are listed later in the ODP Assessment Tool Kit. Step 4 involves assessing the jurisdictions vulnerability based on the assessments of the individual targets.

(3) *CARVER Model* – This model, recently presented by David O'Keefe, NII, at a Briefing for National Emergency Preparedness & Response Partnership Summit II, June 11, 2003, differentiates between:

- Threat analysis is the interpretation of many factors yielding an assessment of “risk” to a person and/or facility by defending forces, and
- Target analysis is the process by which an attacking force chooses the person and/or venue for assault

The model is described as a “target analysis ... conducted by US Govt. Intelligence agencies,” using the acronym CARVER:

- Criticality
- Accessibility
- Recoverability
- Vulnerability
- Espyability (Notoriety)
- Recognizability

Calculations are based on a point system assessing each of the dimensions.

Each of these models has advantages and the purpose here is to suggest the use of some analytical model adopted or developed to fit the needs of the jurisdiction.

AntiTerrorism is preventive in nature. It entails using "Passive and defensive measures... such as education, foreign liaison training, surveillance, and countersurveillance, designed to deter terrorist activities." It is an "integrated, comprehensive approach ... to counter the terrorist threat...." The concept has two phases: proactive and reactive/ The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident. The reactive phase includes the crisis management actions taken to resolve a terrorist incident.¹

Community Policing – a "philosophy of policing, based on the concept that police officers and private citizens working together in creative ways can help solve contemporary community problems related to crime, fear of crime, social and physical disorder, and neighborhood decay."²

Counterintelligence "... information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."³

Counterterrorism is responsive or reactive to terrorist threats or attacks. It entails using "active measures... which incorporate the direct intervention of terrorists groups or the targeting... of terrorist personnel."⁴

CPTED — Crime Prevention Through Environmental Design - a method of reducing the perception of crime, the opportunity for crime, and crime itself by altering the physical environment. Employs Territoriality (creates a sense of ownership), Access Control (increases the perceived risk of crime to potential offenders by restructuring or denying access to crime targets), and Surveillance – (keep potential intruders or attackers under threat of observation).

Design, fabrication, and construction monitoring programs – typically, codes and ordinances that provide for review of new construction, conditional rezoning petitions, development plans, and special exception petitions for the purpose of decreasing the opportunity for crime and increasing the perception of safety.⁵

Fusion Center – an organized structure to coalesce data and information for the purpose of analyzing, linking and disseminating intelligence. A model process is likely to include:

- Extract unstructured data
- Extract structured data

¹ Joint Tactics, Techniques, and Procedures for Antiterrorism Joint Pub 3-07.2. 17 March 1998.

² Trojanowicz, Robert and Bonnie Bucqueroux. (1990). *Community Policing: A Contemporary Perspective*. Cincinnati: Anderson Publishing Co.

³ 50 USC 401a(3)

⁴ Joint Tactics, Techniques, and Procedures for Antiterrorism Joint Pub 3-07.2. 17 March 1998.

⁵ For example, see Plaster, Sherry and Stan Carter. (1993). *Planning for Prevention: Sarasota, Florida's Approach to Crime Prevention Through Environmental Design*. Tallahassee: Florida Criminal Justice Executive Institute.

Fuse structured data

Fused data are then analyzed to generate intelligence products and summaries for tactical, operational, and strategic commanders.

Types of analysis typically conducted in a fusion center include:

- Association Charting
- Temporal Charting
- Spatial Charting
- Link Analysis
- Financial Analysis
- Content Analysis
- Correlation Analysis

Data unprocessed, unanalyzed facts, observations, and raw facts

Force Protection –often used in the military sense to mean a security program designed to protect Service members, civilian employees, family members, facilities, and equipment in all locations and situations.⁶

Information processed fact; reporting with or without analysis. It is often prepared for publication or dissemination in some form and is intended to inform rather than warn or advise.

Intelligence the product of adding value to information and data through analysis. Intelligence is created for a purpose. The process by which analysis is applied to information and data is done to inform policy-making, decision-making, including decisions regarding the allocation of resources, strategic decisions, operations and tactical decisions. Intelligence serves many purposes among which are the identification and elimination of threat sources, the investigation and resolution of threats, the identification and treatment of security risk, the elimination of threat sources, the mitigation of harm associated with risk, preemption, response, preparation and operations related to threats and risks.

Intelligence cycle the process by which information and data is collected, evaluated, stored, analyzed, and then produced or placed in some form for dissemination to the intelligence consumer for use. Cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, consumer,

Intelligence products Intelligence products are the intelligence deliverables. They are the means by which intelligence is communicated to those who will use it. Intelligence products are not limited to written digests or summaries, reports or notes, and also include oral warnings, alerts, advisories or notices given to the consumer when justified. It also includes oral briefings and other presentations made by the intelligence professional within the scope of his or her duties and responsibilities.

⁶ Joint Tactics, Techniques, and Procedures for Antiterrorism Joint Pub 3-07.2. 17 March 1998.

Need-to-know - the determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.⁷

Reasonable Suspicion . . . when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.⁸

Red Team – a technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities, and to anticipate possible modes of attack.

Risk Management Based Intelligence - an approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policy making especially regarding vulnerabilities and counter-measures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability or modality; can be quantitative if a proper data base exists to measure likelihood, impact and calculate risk; can be qualitative, subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations. (See David Schwendiman's *Risk Management Model*, described above.)

Social Capital - Social capital consists of the stock of active connections among people: the trust, mutual understanding, and shared values and behaviors that bind the members of human networks and communities and make cooperative action possible.⁹

Tear Line - the place on an intelligence report (usually denoted by a series of dashes) at which the sanitized, less-classified version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination, in accordance with the "need to know" principle and foreign disclosure guidelines, of the information below the tear line.

Watchout Situations – In fire management and fire service, Watchout Situations are indicators or trigger points that remind firefighters to reanalyze or to re-evaluate their suppression strategies and tactics. The “watchout situations” in the fire service are more specific and cautionary than the “Ten Standard Fire Orders.” In anti-terrorism, the term is used as a metaphor for those observations that can alert trained personnel, not just Firefighters but Law Enforcement, Public Works, Private Security, or anyone, to be more

⁷ CIA Directive 1/7. (1998). Security Controls on the Dissemination of Intelligence Information.

⁸ 28 CFR 23.20(c).

⁹ Cohen, D. and Prusak, L. (2001) *In Good Company. How social capital makes organizations work*, Boston, Ma.: Harvard Business School Press. P. 4.

cautious, more observant, and more likely to report the unusual behavior or activity to the appropriate authorities.

White level inspections – Consistent with OSHA Construction Health and Safety Excellence (CHASE) partnership, private organizations at the “white level” (intermediate level) must implement a comprehensive written safety and health program based on the ANSI A10.38-1991 Guidelines or OSHA's 1989 Safety and Health Program Management Guidelines; meet a variety of training, management, and audit requirements, and have an acceptable safety record.